
**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA	:	<u>CRIMINAL COMPLAINT</u>
	:	
v.	:	Hon. Mark Falk
	:	
LANCE MOORE	:	Mag. No. 11-3651
	:	
	:	FILED UNDER SEAL


I, Jeffrey D. Calandra, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.




Jeffrey D. Calandra, Special Agent
Federal Bureau of Investigation

Sworn to before me, and
subscribed in my presence

July 18, 2011 at
Newark, New Jersey

HONORABLE MARK FALK
UNITED STATES MAGISTRATE JUDGE



Signature of Judicial Officer

ATTACHMENT A

Count One

(Accessing a Protected Computer without Authorization)

On or about April 10, 2011, in Somerset County, in the District of New Jersey and elsewhere, defendant

LANCE MOORE

intentionally accessed a computer without authorization, and exceeded authorized access to a computer, and thereby obtained information from a protected computer, namely the servers of AT&T, and the value of the information obtained exceeded \$5,000.

In violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030 (c)(2)(B)(iii), and 2.

ATTACHMENT B

I, Jeffrey D. Calandra, am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have knowledge of the facts contained in this affidavit based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part.

1. Since in or about July 2011, the FBI has been investigating a data breach at AT&T, Inc. ("AT&T") that resulted in the theft of confidential business information from AT&T. As summarized below, the investigation has revealed that defendant LANCE MOORE ("MOORE") was responsible for this data breach and the associated theft of confidential AT&T business information.

A. AT&T, Convergys, and Defendant MOORE

2. AT &T is a global communications provider, headquartered in Dallas, Texas, with over 266,000 employees worldwide. AT&T's Global Network Operations Center ("GNOC") is the largest command-and-control center of its kind in the world, and is located in Bedminster, New Jersey. GNOC staff monitor and manage the data and voice traffic flowing across AT&T's domestic and global networks twenty-four hours a day, seven days a week.

3. AT&T Mobility LLC is a wholly owned subsidiary of AT&T that provides wireless services to approximately 97.5 million subscribers in the United States, Puerto Rico and the U.S. Virgin Islands.

4. Convergys Corporation ("Convergys"), headquartered in Cincinnati, Ohio, is a global leader in relationship management services, consulting and professional services, billing services, and self-care technology. Convergys has over 70,000 employees, and offices throughout North America. Its clients include companies in the telecommunications, financial services, technology, government, and employee care markets. AT&T is a Convergys customer, and Convergys maintains an office site at AT&T's offices in Bedminster, New Jersey. Among other things, Convergys provides customer care call center services to AT&T Mobility customers.

5. On or about August 23, 2010, Convergys hired MOORE as a customer support contractor to work on the AT&T Mobility account from Convergys's office located at 4201 Del Rey Blvd, Las Cruces, New Mexico, 88012. MOORE was responsible for answering calls from AT&T Mobility customers, and troubleshooting their problems.

6. To facilitate his work, MOORE was assigned a unique username and maintained a secure password that he created that permitted him to log onto and access Convergys's computer network. In addition, MOORE was given Virtual Private Network ("VPN") access to certain

AT&T computer networks. A VPN is a network that provides remote offices or individual users with secure access to an organization's computer networks – in this case AT&T's networks – using the Internet. MOORE was assigned a unique username and maintained a secure password that he created that permitted him to access certain parts of AT&T's computer networks using VPN.

B. The Data Breach

7. On or about April 16, 2011, AT&T's Chief Security Office ("CSO") Team, located in Bedminster, New Jersey, discovered that AT&T confidential information may have been misappropriated and posted on a public file hosting site, Fileape.com. The CSO Team immediately began conducting an initial assessment of this data breach, employing additional resources from AT&T's Bedminster, New Jersey office.

8. Fileape.com is a public file hosting site that prides itself on preserving user anonymity. For example, Fileape.com's Terms of Service page states the following:

- "Fileape isn't just another file host. Well, okay, it is. But compared to other filehosts, fileape takes a strict stance on privacy. Summarized: we protect you"
- "If you upload a file, we do not store your IP Address";
- "If you register, we do not store your IP Address. You don't even have to provide us with an email";
- "If you download a file, you are not logged"; and,
- "If you purchase a premium account, unless you've provided us with an email account to send a receipt, we will not store any information about you."

9. The investigation has confirmed that AT&T confidential information was, indeed, posted on Fileape.com on or about April 10, 2011, and made available for public download. This information (hereinafter the "AT&T Confidential Information") included thousands of spreadsheets, Microsoft Word documents, Microsoft PowerPoint presentations, image files, PDF files, applications, and other files largely concerning AT&T's plans related to its 4G data network and LTE ("Long Term Evolution") mobile broadband network, among other topics.

10. The AT&T Confidential Information that was publicly disclosed on Fileape.com on or about April 10, 2011 had been stored on AT&T's secured servers, which are protected computers as defined in Title 18, United States Code, Section 1030(e)(2). In addition, based on interviews of AT&T personnel, the value of the disclosed AT&T Confidential Information exceeded \$5,000.

C. The AT&T Internal Investigation, and Identification of Defendant MOORE

11. On or about April 18, 2011, AT&T began an internal investigation concerning the release of the AT&T Confidential Information. To this end, AT&T investigators obtained and reviewed system and network information, including network logs. The review of network logs

revealed that on or about April 10, 2011 an Internet Protocol address (or "IP address") on the AT&T Mobility network accessed Fileape.com. Additional investigation revealed that the IP address in question was associated with an AT&T Mobility server accessed by Convergys's contractors working on the AT&T Mobility account, and that usernames associated with approximately 19 Convergys contractors, including MOORE, were connected to that server at the time the AT&T Confidential Information was uploaded to Fileape.com on or about April 10, 2011.

12. AT&T investigators subsequently compared the usernames of the 19 Convergys contractors with a list of usernames that accessed and downloaded the AT&T Confidential Information on the AT&T Mobility Server. Only defendant MOORE's AT&T username accessed both Fileape.com, and the servers containing the AT&T Confidential Information. Indeed, MOORE's username was used to download the AT&T Confidential Information shortly before that same information was uploaded to Fileape.com and made publicly available.

13. In addition, a review of internet usage reports reveal that shortly before the upload of the AT&T Confidential Information to Fileape.com, there were a number of Google searches for uploading files, file hosting, and uploading zip files associated with MOORE's AT&T username. Based on my training and experience, these searches are consistent with the type of services provided by Fileape.com, and the manner in which the AT&T Confidential Information was uploaded to Fileape.com.

14. A review of Convergys's records also confirmed that MOORE was present and working at Convergys's Las Cruces, New Mexico office on or about April 10, 2011 at the time the AT&T Confidential Information was accessed, downloaded, and uploaded to FileApe.com, as described in paragraphs 11 through 13, above. Furthermore, Convergys network logs indicated that MOORE's username was used to access Fileape.com and pastebin.com, a similar file hosting site, on multiple occasions following the April 10, 2011.

15. On or about May 19, 2011, an AT&T investigator interviewed MOORE concerning the above-described conduct and data breach. Although MOORE denied any involvement in accessing and disseminating the AT&T Confidential Information, he acknowledged that he was aware of AT&T's network security policies, and that he was not permitted to share his username and password with anyone, and, in fact, had not done so.

16. On or about May 19, 2011, MOORE was escorted from Convergys's Las Cruces, New Mexico office, and his network access was disabled. Convergys subsequently terminated his employment.

17. Based on interviews of witnesses in this case, MOORE was authorized to access various portions of the AT&T's network during the course of his employment, but his access of the AT&T Confidential Information, and subsequent release of the same, exceeded his authorization.

18. Finally, on or about June 25, 2011, the computer hacking group LulzSec publicized that they had obtained the AT&T Confidential Information and re-circulated it on the Internet.